

## 【資安訊息】請強化網路電話設備之管控機制，避免因不安全之設定而成為詐騙活動之工具

### 教育機構ANA通報平台

發佈編號	TACERT-ANA-2024102101100303	發佈時間	2024-10-21 13:30:03
事故類型	ANA-漏洞預警	發現時間	2024-10-19 13:30:03
影響等級	低		

[主旨說明:]【資安訊息】請強化網路電話設備之管控機制，避免因不安全之設定而成為詐騙活動之工具

#### [內容說明:]

轉發 國家資安資訊分享與分析中心 NISAC-400-202410-00000030

資安院接獲外部情資，近期發現網路電話交換機，如透過公開網路存取，且存在弱密碼之弱點，將導致設備遭犯罪集團駭侵控制，且用於惡意盜打與詐騙活動。

(1) 網通設備若預設開啟遠端登入 (Telnet)，當置於網際網路上，且未使用防火牆設備保護，則容易遭受駭客攻擊。

(2) 網通設備遭暴力破解取得帳號密碼，將被修改設定做為詐騙集團盜打詐騙電話之用 請各會員參考建議措施加強網路電話相關設備之清查與管控，有關遠端管理作業應遵循「原則禁止，例外開放」之原則，並妥善規劃網路架構，避免網通設備暴露於公開網路。

情資分享等級：WHITE(情資內容為可公開揭露之資訊)

此訊息僅發送到「區縣市網路中心」，煩請貴單位協助公告或轉發

#### [影響平台:]

無

#### [建議措施:]

清查轄下是否使用網路電話相關設備，並對其加強下列安全管控措施：

1. 進行帳號清查作業，落實密碼複雜度、定期變更等密碼安全管控。
2. 關閉不必要的服務與通訊埠。
3. 停用或加強管控遠端管理功能，遵循「原則禁止，例外開放」之原則。
4. 重新檢視網路架構，網通設備應妥善調整至防火牆。
5. 系統軟體更新至最新版本，如已逾產品生命週期則請更換設備。

#### [參考資料:]

(此通報僅在於告知相關資訊，並非為資安事件) · 如果您對此通報的內容有疑問或有關於此事件的建議，歡迎與我們連絡。

教育機構資安通報應變小組

網址：<https://info.cert.tanet.edu.tw/>

專線電話：07-5250211

網路電話：98400000

E-Mail：[service@cert.tanet.edu.tw](mailto:service@cert.tanet.edu.tw)